(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 July 2003 (24.07.2003)

PCT

(10) International Publication Number
WO 03/060674 A1

(51) International Patent Classification[7]: G06F 1/00, H04N 1/44, H04K 1/00

(21) International Application Number: PCT/IB02/05423

(22) International Filing Date: 13 December 2002 (13.12.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02075178.0 17 January 2002 (17.01.2002) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **STARING, Antonius, A., M.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **VAN DIJK, Marten, E.** [NL/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **TUYLS, Pim, T.** [BE/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

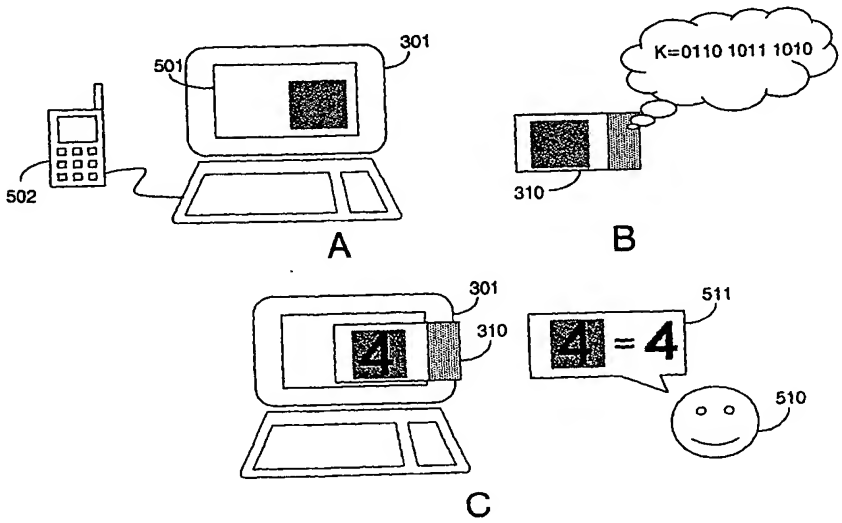
(74) Agent: **GROENENDAAL, Antonius, W., M.**; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURE DATA INPUT DIALOGUE USING VISUAL CRYPTOGRAPHY



(57) Abstract: A method of secure transmission and reception of a message from a user. An image (320) representing a plurality of input means, e.g. an image of a keypad, is generated and encoded. The image is encoded using visual cryptography using a key sequence stored in a decryption device (310) as randomization. The randomized image is transmitted to the client device (301), where it is displayed on a first display (501) .The randomization is displayed on a second display (311) .Superimposing the first and second displays reveals the image. The client device (301) allows the user to select particular spots on the first display (501) that correspond to the location of particular input means on the reconstructed image. The coordinates of these spots are transmitted back to the server (300), which can translate them to the particular input means selected by the user. The message is then constructed as the input symbol represented by the particular input means.

WO 03/060674 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

PCT/IB 02/05423

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 H04N1/44 H04K1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04N H04K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 806 230 A (FRANCE TELECOM) 14 September 2001 (2001-09-14)	7,8
A	page 4, line 14 -page 6, line 22; figure 2	1,5,9,10
A	US 6 209 102 B1 (HOOVER DOUGLAS) 27 March 2001 (2001-03-27) cited in the application column 2, line 5 -column 4, line 7; figures 1,3	1,3,4,9
A	NAOR M ET AL: "Visual cryptography" ADVANCES IN CRYPTOLOGY. EUROCRYPT, XX, XX, 12 May 1994 (1994-05-12), pages 1-12, XP002205767 cited in the application page 1; figure 1	1,2,5

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 April 2003	22/04/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Seytter, F

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	CA 2 214 190 A (BLOM MICHAEL ERNEST) 15 April 1999 (1999-04-15) Sections 2.1, 4.1, 5.2, 5.3 ---	1,3-6,9, 10
A	US 5 428 349 A (BAKER DANIEL G) 27 June 1995 (1995-06-27) ---	
A	US 5 970 146 A (BIEDERMANN DAVID A ET AL) 19 October 1999 (1999-10-19) -----	

INTERNA[redacted]AL SEARCH REPORT

patent family members

PCT/IB 02/05423

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
FR 2806230	A	14-09-2001	FR	2806230 A1	14-09-2001
US 6209102	B1	27-03-2001	AU	3490100 A	29-08-2000
			CA	2359119 A1	17-08-2000
			EP	1181643 A1	27-02-2002
			JP	2002536762 T	29-10-2002
			NO	20013932 A	09-10-2001
			WO	0048076 A1	17-08-2000
CA 2214190	A	15-04-1999	CA	2214190 A1	15-04-1999
US 5428349	A	27-06-1995	NONE		
US 5970146	A	19-10-1999	NONE		